UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC.,

Plaintiff,

v. Case No. 22-cv-00187

SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1-50,

Defendants.

DECLARATION OF BRUCE W. PIXLEY

BRUCE W. PIXLEY, under penalty of perjury and pursuant to 28 U.S.C. § 1746, declares the following to be true and correct:

I. Background

1. My name is Bruce W. Pixley. I provide this declaration in support of Moog Inc.'s ("Moog") Opposition to defendant Skyryse, Inc.'s Motion to Enter Source Code Protocol. I am over the age of 18 years. I have personal knowledge of the matters set forth herein and if called as a witness, I could and would competently testify as to all facts set forth herein.

2. I am the Managing Member of Pixley Forensics Group LLC. My responsibilities include assisting corporate clients and law firms in investigations and disputes involving forensic accounting issues, electronic discovery, theft of intellectual property, and computer forensic investigations. In this capacity, I manage teams of forensic examiners and use a variety of technologies to perform data acquisition and analysis of this information.

3. Since 2001, I have served as a lead instructor of computer forensics, Internet investigations, and network intrusion courses for the California Department of Justice's

Advanced Training Center. Additionally, I have been employed as a Master Instructor at Guidance Software, which developed the EnCase computer forensic software. As an instructor, I have taught for over 2,000 hours on the subjects of computer forensics and high-tech investigations. I have developed course training materials and wrote manuals for computer forensic courses such as Advanced Internet Examinations and Network Intrusion Investigations.

4. I possess three professional certifications for my fields of work. I possess the Certified Information Systems Security Professional (CISSP) certification and the GIAC Certified Forensic Analyst (GCFA) certification, which are both ANSI ISO accredited credentials, and the EnCase Certified Examiner certification.

5. Since 2003, I have been retained as a computer forensic examiner and subject matter expert in both criminal and civil matters. I have been qualified as an expert witness in both state and federal courts and testified about the foundation of computer forensics, Windows and Mac operating systems, chat software, Internet and network operations, e-mail, peer-to-peer file sharing, digital photography, recovery of deleted data, and Trojan viruses.

6. I have been retained by Sheppard, Mullin, Richter & Hampton LLP, counsel for Moog Inc. ("Moog" or "Company") to conduct a forensic analysis of: 1) certain company-issued laptop computers and external storage drives for any evidence of the exfiltration of Company data; and 2) electronic devices and data produced by the Defendants in this case which are in the possession of a third party forensics vendor, iDiscovery Solutions ("iDS").

II. The Court's Inspection Protocol Is Secure

7. Pursuant to the procedures set forth in the Protective Order entered in this case (ECF 89) and the Inspection Protocol (ECF 96-02), I have been granted access to certain electronic devices turned over to iDS through inspection laptops and iDS's remote virtual machine software.

8. I have reviewed Skyryse's Motion to Enter Source Code Protocol and Skyryse's proposed second source code protocol attached as Exhibit "A" thereto. (ECF 213). I understand that in its motion, Skyryse is raising a number of purported security concerns regarding the existing Inspection Protocol.

9. In my professional experience and having inspected devices and materials via iDS pursuant to the Inspection Protocol for several weeks, the Inspection Protocol is extremely secure. The security measures that have been placed in the iDS Protocol provides a multi-layered security approach to protect and secure data provided by both parties. The security measures include the following:

- The review process requires the strict use of a locked-down Inspection Laptop. No personal or unauthorized devices are allowed connectivity to the Inspection Laptop.
- The virtual machines that have been dedicated to the review process are powered off until iDS intentionally starts a review session with an Authorized Reviewer.
- Authorized Reviewers must start an online video-based meeting with iDS using their assigned Inspection Laptop. iDS confirms the identity of each Authorized Reviewer at the start of each session. This entire online meeting is recorded in video format by iDS. Since iDS controls this access, no one can access the review platform until permission has been provided.

- Once an Authorized Reviewer has been granted access, a Reviewer is unable to export any data. The Reviewer must follow the procedures described in the Court's Inspection Protocol, which is controlled by iDS. Outside Internet-based access has been blocked through effective firewall rules.
- At the conclusion of the Authorized Reviewers sessions, the review platform is effectively powered off by IDS to prevent any unauthorized access.

10. In my decades of experience in working with defendants, plaintiffs, and as a third-party neutral, this is the most comprehensive protocol I have seen established for both parties to be able to conduct a thorough review of all data in a secure and controlled environment.

III. The Inspection Protocol Does Not Permit Internet Access

11. While it appears that the majority of Skyryse's purported security concerns regarding the Inspection Protocol are general, and not based on any specific examples, I understand one specific concern is regarding internet access: "under the iDS Protocol, which unquestionably allows for internet access, Moog has already installed standard web browsers, through which one could make source code available over the Internet. While the iDS Protocol attempts to partially restrict internet access, it does so by requiring the parties rely entirely on iDS to create a flawless system." (ECF 213 at p. 6). Skyryse's claims are not correct, and the Inspection Protocol does not permit any type of internet access during inspection.

12. Each Inspection laptop, which was configured and locked down by iDS per the Inspection Protocol, is limited to two applications that can be used by an Authorized Reviewer: Microsoft Remote Desktop and Zoom.

13. The Microsoft Remote Desktop application is configured to connect to specific Remote Desktop sessions ("Remote Session") hosted by iDS. These hosted Remote Sessions are

intentionally turned off by iDS and inaccessible until they are powered on by iDS. iDS keeps the Remote Sessions powered off until iDS has opened a video-based Zoom meeting with an Authorized Reviewer.

14. The Remote Sessions do not allow outside Internet access as outside Internet access has been blocked by IDS. While a Remote Session may have a web browser installed, an Authorized Reviewer cannot access Internet-based content. This includes, but is not limited to, a complete prohibition against access to web sites, print services, cloud storage, email, chat communications, and file transfer services.

15. The only method for an Authorized Reviewer to export content from the Remote Session is to place notes and/or work product in a document, such as Word or Excel. The file name and path of the document has to be submitted to iDS and only iDS can export the document to counsel, pursuant to Section III.F.2 of the Inspection Protocol.

16. Skyryse's claims that the Inspection Protocol allows for internet access is simply not correct. Each Remote Session is running the Windows 10 Pro operating system and Microsoft embedded their web browser called Edge into the operating system. However, even though a web browser may exist, it cannot access any outside Internet-based resources. iDS did not simply "attempt" to partially restrict Internet access; iDS did, in fact, fully restrict Internet access.

17. I further note that in its Motion, Skyryse did not provide any specific example of how Internet access is permitted on the iDS system. Skyryse merely alluded to it by stating that a web browser was installed and, therefore, that must equate to actual Internet access. However, as soon as an Authorized Reviewer opens the web browser, the reviewer sees that any website

cannot be accessed. Again, this is due to iDS successfully blocking outside Internet-based content.

I declare that the foregoing is true and correct under penalty of perjury under the laws of the United States of America.

Dated: August 17, 2022

Bruce W. Pixley